UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/762,364	01/23/2004	Roger Maitland	Q102939	4471

23373 7590 09/15/2011
SUGHRUE MION, PLLC
2100 PENNSYLVANIA AVENUE, N.W.
SUITE 800
WASHINGTON, DC 20037

EXAMINER	
TRAN, ELLEN C	

ART UNIT	PAPER NUMBER
2433	

NOTIFICATION DATE	DELIVERY MODE
09/15/2011	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

sughrue@sughrue.com
PPROCESSING@SUGHRUE.COM
USPTO@SUGHRUE.COM

UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

Application Number: 10/762,364
Filing Date: January 23, 2004
Appellant(s): MAITLAND ET AL.

David J. Cushing
Reg. No. 28,703
For Appellant

EXAMINER'S ANSWER

This is in response to the appeal brief filed 18 May 2011 appealing from the Office action mailed 4 March 2009.

(1) Real Party in Interest

The examiner has no comment on the statement, or lack of statement, identifying by name the real party in interest in the brief.

(2) Related Appeals and Interferences

The examiner is not aware of any related appeals, interferences, or judicial proceedings which will directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

(3) Status of Claims

The statement of the status of claims contained in the brief is correct.

(4) Status of Amendments After Final

The examiner has no comment on the appellant's statement of the status of amendments after final rejection contained in the brief.

(5) Summary of Claimed Subject Matter

The examiner has no comment on the summary of claimed subject matter contained in the brief.

(6) Grounds of Rejection to be Reviewed on Appeal

The examiner has no comment on the appellant's statement of the grounds of rejection to be reviewed on appeal. Every ground of rejection set forth in the Office action from which the appeal is taken (as modified by any advisory actions) is being maintained by the examiner except for the grounds of rejection (if any) listed under the subheading "WITHDRAWN REJECTIONS." New grounds of rejection (if any) are provided under the subheading "NEW GROUNDS OF REJECTION."

(7) Claims Appendix

The examiner has no comment on the copy of the appealed claims contained in the Appendix to the appellant's brief.

(8) Evidence Relied Upon

Kim et al. World Intellectual Property Organization No. WO 03/050784 {Note in the eDAN application this is the foreign reference (FOR) dated 11 July 2007}

Luyster U.S. Patent No. 6,751,319

3GPP TS 35.202 v3.1.1 Release 1999 {Note in the eDAN application this is the NPL reference dated 23 May 2008}

Weybrew et al. U.S. Patent No. 6,931,511

(9) Grounds of Rejection

The following ground(s) of rejection are applicable to the appealed claims:

Claims 74-79, are rejected under 35 U.S.C. 103(a) as being unpatentable over Kim et al. World Intellectual Property Organization No. WO 03/050784 (hereinafter Kim) International Filing Date 17 April 2002 in view of Luyster U.S. Patent No. 6,751,319 (hereinafter Luyster).

As per the first limitation of claim 74, A method comprising the step of, responsive to a plurality of inputs, each input being defined by at least one bit, for each input of the plurality of inputs and in parallel with other inputs of the plurality of inputs" is taught in Kim on page 9, lines 8-31, note the first pipeline stores upper 16-bit data of the 32-bit input. The upper 16-bit data is interpreted to be equivalent to a first set of bits, the lower 16-bit data is interpreted be equivalent to the second set, and simultaneously is interpreted to be equivalent to in parallel;

As per the second limitation, "looking-up a look-up table having a plurality of elements using the at least one bit that define the input to obtain an output" however Luyster teaches that the s-box or lookup table is used with encryption in col. 17, lines 30-51, therefore it is understood the "s-boxes" in Kim are the same as "look-up tables".

Regarding claim 75, this claim is directed to the apparatus executing the method of claim 74; therefore it is rejected along similar rationale.

Regarding claim 76, this claim is directed to an article of manufacture executing the method of claim 74; therefore it is rejected along similar rationale.

Claims 1, 2, 5, 6, 11-13, 16, 21-28, 30, 31, 33-42, 44, 45, 47-73, and 77-79, are rejected under 35 U.S.C. 103(a) as being unpatentable over Kim et al. World Intellectual Property Organization No. WO 03/050784 (hereinafter Kim) International Filing Date 17 April 2002 in view of Luyster U.S. Patent No. 6,751,319 (hereinafter Luyster) in further view of 3GPP TS 35.202 v3.1.1 Release 1999 (hereinafter 3GPP).

As per the first limitation of claim 1, "A method comprising responsive to a plurality of inputs, each input being defined by a first set of bits and a second set of at least one bit, for each input of the plurality of inputs and in parallel with other inputs of the plurality of inputs:" is taught in Kim on page 9, lines 8-31, note the first pipeline stores upper 16-bit data of the 32-bit input. The upper 16-bit data is interpreted to be equivalent to a first set of bits, the lower 16-bit data is interpreted be equivalent to the second set, and simultaneously is interpreted to be equivalent to in parallel;

As per the second limitation, "for each of a plurality of look-up tables each having a plurality of elements, looking-up one of the plurality of elements of the look-up table using the first set of bits that define the input to obtain an output, the output from each of the plurality of look-up tables collectively comprising a set of corresponding outputs" however Luyster teaches that the s-box or lookup table is used with encryption in col. 17, lines 30-51;

As per the third limitation, "and selecting a corresponding output from the set of corresponding outputs using the second set of a least one bit that defines the input" however '3GPP teaches on page 11-12 sections 4.4 and 4.5 that the output from the first bit string are utilized for inputs to the second string (or second set of at least one bit). Note the s-box is interpreted equivalent to the lookup tables.

Regarding claim 2, "wherein the plurality of elements of each look-up table collectively comprise a combined table of elements each having a pre-determined value obtained using an S7 function" is taught in Kim page 11, lines 4-10.

Regarding claim 5, "wherein for each of the plurality of inputs, the second set of at least one bit that defines the input comprises one bit and the set of corresponding outputs comprises two corresponding outputs, and wherein for each of the plurality of inputs the selecting comprises: selecting one of the two outputs using the one bit of the at least one bit that defines the input" is taught in Kim page 4, lines 30-35.

Regarding claim 6, "wherein for each of the plurality of inputs, the second set of at least one bit that defines the input comprises at least two bits, and wherein for each of the plurality of inputs the selecting comprises: successively performing a selection on a remaining number of corresponding outputs of the set of corresponding outputs for each bit of the at least two bits, the

number of corresponding outputs remaining being equal to all of the corresponding outputs of the set of corresponding outputs a first time the selection is performed, the selection being replacing the remaining number of corresponding outputs with a selection of half of the remaining number of outputs using a respective bit of the at least two bits, the selection of half of the remaining number of outputs being the number of remaining outputs for the next time the selection is performed" is shown in Kim page 6, lines 8-29.

Regarding claim 11, "applied in ciphering data in a Kasumi implementation" is taught in Kim page 2, lines 25-33.

Regarding claim 12, this claim is directed to the apparatus executing the method of claim 1; therefore it is rejected along similar rationale.

Regarding claims 13 and 16, these claims contain substantially similar subject matter as claims 2, 5, and 6; therefore they are rejected along similar rationale.

As per the first limitation of claim 21, "A method comprising: responsive to a plurality of inputs, each input being defined by a first plurality of bits, for each input of the plurality of inputs and in parallel with other inputs of the plurality of inputs" is taught in Kim on page 9, lines 8-31, note the first pipeline stores upper 16-bit data of the 32-bit input. The upper 16-bit data is interpreted to be equivalent to a first set of bits, the lower 16-bit data is interpreted be equivalent to the second set, and simultaneously is interpreted to be equivalent to in parallel;

As per the second limitation, "selecting a respective subset of bits of the first plurality of bits that define the input, the bits of the respective subset of bits comprising fewer bits than the

first plurality of bits of the input" is shown on page 9, lines 13-31, note of the 32 input bits 16 are separated and applied to 9-bit and 7-bit of the FI function defined in the KASUMI encryption;

As per the third limitation, "and looking-up an element of the plurality of elements of the look-up table using the subset of bits to obtain an output"; however Luyster teaches that the s-box or lookup table is used with encryption in col. 17, lines 30-51.

As per the fourth limitation, "and for each of a plurality of look-up tables each having a plurality of elements" and "and combining the outputs obtained from the plurality of look-up tables to obtain at least one bit" however '3GPP teaches on page 11-12 sections 4.4 and 4.5 that the output from the first bit string are utilized for inputs to the second string (or second set of at least one bit). Note the s-box is interpreted equivalent to the lookup tables.

Regarding claim 22, "wherein for each input of the plurality of inputs, the outputs obtained from the plurality of look-up tables each comprise a second plurality of bits, the second plurality of bits comprising fewer bits than the first plurality of bits of the input" is shown in Kim page 10, lines 9-15.

Regarding claim 23, "wherein for each input of the plurality of inputs, the at least one bit comprises a third plurality of bits, the third plurality of bits comprising the same number of bits as the first plurality of bits of the input" is shown in Kim page 10,
lines 9-15.

Regarding claim 24, "wherein for at least one look-up table of the plurality of look-up tables, for each input the selecting comprises manipulating at least one of the plurality of bits that

define the input using at least one of a bit rotation instruction and a bit shifting instruction" is disclosed in Kim page 6, lines 1-29.

Regarding claim 25, "wherein for each of the at least one look-up table, for each input the manipulating at least one of the first plurality of bits comprises ordering the respective subset of bits of the input as least significant bits" is taught in Kim page 9,
lines 7-31.

Regarding claim 26, "wherein each element of the plurality of elements of each look-up table has a pre-determined value" however Luyster teaches loading predetermined values into tables in col. 38, lines 24-36.

Regarding claim 27, "wherein for each input of the plurality of inputs the first plurality of bits and the third plurality of bits each comprise 9 bits, the pre-determined value of each of the plurality of elements of each of the plurality of look-up tables is obtained from a partial evaluation of an S9 function" is shown in Kim page 9, line 32 through page 10, line 8.

Regarding claim 28, "wherein for each look-up table of the plurality of look-up tables, the pre-determined value of each of the plurality of elements of the look-up table is a function of a number being definable by a bit sequence of one of 4 and 5 bits" is disclosed in Kim page 13, lines 9-16.

Regarding claim 30, "wherein for each input of the plurality of inputs, the combining comprises performing a plurality of exclusive-OR operations on the outputs obtained from the plurality of look-up tables for the input" is taught in Kim page 9,
lines 9-31.

Regarding claim 31, "wherein for each input of the plurality of inputs, the combining comprises manipulating the second plurality of bits of at least one output of the outputs obtained from the plurality of look-up tables for the input using one of a bit shifting instruction and a bit rotation instruction" is shown in Kim page 9, lines 9-31.

Regarding claim 33, "wherein for each input of the plurality of inputs, the combining comprises: for a first output of the outputs obtained from the plurality of look-up tables for the input, manipulating the second plurality of bits of the first output using one of a bit rotation instruction and a bit shifting instruction; and for a second output of the outputs obi;aired from the plurality of look-up tables for the input, performing one of the plurality of exclusive-OR operations on the second output and the first output to obtain a third output having a fourth plurality of bits" is disclosed in Kim page 9, lines 9-31.

As per the first limitation of claim 34, "wherein for each input, the bits of the second plurality of bits of each respective subset of bits of the first plurality of bits of the input have a pre-determined order and are each used for obtaining a respective one of the third plurality of bits, the outputs obtained from the look-up tables collectively comprising at least one group of outputs each having at least two outputs of the outputs obtained from the look-up tables" however Luyster teaches lookup tables in col. 15, lines 48-55;

As per the second limitation, "for each group of outputs of the at least one group of outputs the at least two outputs in the group of outputs having bits used for determining a common subset of bits of the third plurality of bits, the combining comprising: for each group of outputs of the at least of group of outputs, combining the at least two outputs of the group of

outputs using at least one of the plurality of exclusive-OR operations" is shown in Kim page 5, lines 10-36.

Regarding claim 35, this claim is directed to the apparatus executing the method of claim 21; therefore it is rejected along similar rationale.

Regarding claims 36-42, 44, 45, 47, and 48, these claims contain substantially similar subject matter as claims 22-28, 30, 31, 33, and 34; therefore they are rejected along similar rationale.

Regarding claim 49, this claim is directed to an article of manufacture of the method of claim 1; therefore it is rejected along similar rationale.

Regarding claim 50, this claim is directed to an article of manufacture of the method of claim 21; therefore it is rejected along similar rationale.

As per the first limitation of claim 51, "A method comprising, responsive to N K_{in}-bit inputs: performing bit reordering on the N K_{in}-bit inputs to produce M parallel sets of outputs wherein N and K_{in} are integers satisfying N, $K_{in} \geq 2$" is taught in Kim on page 6, lines 1-29, Kim teaches the Kasumi algorithm, the Kin and Kout bits as well as the bit rotation on shown in FIG. 2 ;

As per the second limitation, "an ith set of outputs of the M parallel sets of outputs containing N sets of bits $L_{i,in}$ bits in length with i and $L_{i,in}$ being integers satisfying i=1 to M and $1 \leq L_{i,in} < K_{in}$, the ith set of outputs defining a respective subset of the K_{in} bits of the inputs" is taught in Kim on page 9, lines 8-31, note the first pipeline stores upper 16-bit data of the 32-bit input. The upper 16-bit data is interpreted to be equivalent to Li, in a first set of bits, the lower

16-bit data is interpreted be equivalent to the second set, and simultaneously is interpreted to be equivalent to in parallel;

As per the third limitation, "for each parallel set of outputs, performing a parallel lookup table operation to generate a corresponding parallel set of outputs containing N outputs, each being associated with a respective one of the N K_{in}-bit inputs and each being $L_{i,out}$ bits in length" however Luyster teaches that the s-box or lookup table is used with encryption in col. 17, lines 30-51.

As per the fourth limitation, "$L_{i,out}$ being an integer satisfying $L_{i,out} \geq 1$; and for each of the N K_{in}-bit inputs, generating a respective output by performing a bit combining operation on the outputs from the parallel look-up table operations associated with the input" however '3GPP teaches on page 11-12 sections 4.4 and 4.5 that the output from the first bit string are utilized for inputs to the second string (or second set of at least one bit). Note the s-box is interpreted equivalent to the lookup tables.

Regarding 52, "wherein for each of the N K_{in}-bit inputs, the generating comprises performing a bit manipulation on the outputs of the parallel look-up table operations associated with the input" is disclosed in Kim page 6, lines 1-29.

Regarding 53, "wherein the bit combining operations are implemented in parallel" is taught in Kim on page 9, lines 8-31, note simultaneously is interpreted to be equivalent to in parallel.

Regarding claim 54, "wherein for each of the N K_{in}-bit inputs the respective output generated K_{out} bits, K_{out} being an integer satisfying $K_{out} \geq 1$, and wherein in performing the bit permutation/reordering on the N K_{in}-bit inputs, the ith set of outputs defining the respective

subset of the K_{in} bits of the inputs is selected such that the respective subset of the K_{in} bits effects only a defined maximum number $Pi< K_{out}$ bits of the respective outputs wherein Pi is an integer" is disclosed in Kim page 6, lines 1-29.

As per the first limitation of claim 55, "A method of generating a plurality of outputs according to a ciphering algorithm which for each of the plurality of outputs operates on a respective input using a respective key" is taught in Kim page 6, lines 5-18, note Kim teaches that the key registers store keys that are rotated;

As per the second limitation, "responsive to a plurality of first inputs each being associated with one of the respective inputs, for each first input and in parallel with other first inputs of the plurality of first inputs:" is taught on page 9, lines 8-31, note simultaneously is interpreted to be equivalent to in parallel;

As per the third limitation, "generating an output by looking up at least one look-up table using the input, each look-up table having a plurality of elements" however Luyster teaches that the s-box or lookup table is used with encryption in col. 17, lines 30-51.

As per the fourth limitation, "the ciphering algorithm comprising a plurality of rounds in which functions are evaluated, the method comprising, for at least one function of the functions of at least one of the plurality of rounds:" however 3GPP teaches that the Kasumi algorithm is a plurality of functions that are evaluated in the round functions see page 10, section 4.1.

Regarding claim 56, "wherein the ciphering algorithm is a Kasumi algorithm" is taught in Kim page 2, lines 25-33.

As per the first limitation of claim 57, "wherein for a function of a certain type of the at least one function the at least one look-up table comprising a plurality of look-up tables and the

output from each of the plurality of look-up tables collectively comprising a set of corresponding outputs" however Luyster teaches that the s-box or lookup table is used with encryption in col. 17, lines 30-51;

As per the second limitation, "each first input of the plurality of first inputs being defined by a first set of bits and a second set of at least one bit, the method comprising for each first input of the plurality of first inputs and in parallel with the other first inputs of the plurality of first inputs:" is taught in Kim on page 9, lines 8-31;

As per the third limitation, "selecting a corresponding output from the set of corresponding outputs using the second set of at least one bit that defines the input" is shown in Kim page 6, lines 8-29.

Regarding claim 58, "wherein the ciphering algorithm is a Kasumi algorithm and the function of a certain type is an S7 function" is taught in Kim page 11, lines 4-10.

As per the first limitation of claim 59, "wherein, for a function of a certain type of the at least one function the at least one look-up table comprises a plurality of look-up tables and each first input of the plurality of first inputs is defined by a first plurality of bits, the method comprising:" however Luyster teaches that the s-box or lookup table is used with encryption in col. 17, lines 30-51;

As per the second limitation, "for each first input of the plurality of first inputs and in parallel with the other first inputs of the plurality of first inputs, and for each of the plurality of look-up tables: selecting a respective subset of bits of the first plurality of bits that define the first input, the bits of the respective subset of bits comprising fewer bits than the first plurality of bits

of the first input, the look-up table being looked up using the subset of bits to obtain the output" is shown in Kim page 6, lines 8-29;

As per the third limitation, "and combining the outputs obtained from the plurality of look-up tables to obtain at least one bit" is taught in Kim page 2, lines 25-33.

Regarding claim 60, "wherein the ciphering algorithm is a Kasumi algorithm and the function of a certain type is an S9 function" is taught in Kim page 11, lines 4-10.

Regarding claim 61, "wherein the at least one round comprises the plurality of rounds and wherein for each round the at least one function comprises six S7 functions and six S9 functions, the method further comprising for each function of the plurality of functions other then the at least one function, and responsive to a plurality of second inputs each being associated with one of the respective inputs, and in parallel with other second inputs of the plurality of second inputs: generating an output according to the function using the input" is shown in Kim page 11, lines 4-36.

Regarding claim 62, "further comprising, for each output of the plurality of outputs and in parallel with other outputs of the plurality of outputs: combining the output with input data to generate ciphered data" is taught in Kim on page 9, lines 8-31.

Regarding claim 63, "wherein the combining comprises performing an exclusive-OR operation" is taught in Kim page 9, lines 9-31.

Regarding claim 64, this claim is directed to the apparatus executing the method of claim 55; therefore it is rejected along similar rationale.

Regarding claims 65-72, these claims contain substantially similar subject matter as claims 56-63; therefore they are rejected along similar rationale.

Regarding claim 73, this claim is directed to an article of manufacture of the method of claim 55; therefore it is rejected along similar rationale.

Regarding claim 77, the following is not explicitly taught in the combination of Kim and Luyster: "wherein the look-up table outputs corresponding to the plurality of inputs comprise a set of outputs, and said method further comprises the step of selecting one of said outputs in response to at least one additional bit included in at least one of said plurality of inputs" however 3GPP teaches that the two S-boxes, i.e. lookup tables to be implemented in combinational logic to make output in response to bit selection in section 4.5 on page 12.

Regarding claims 78 and 79, these claims contain substantially similar subject matter as claim 77; therefore they are rejected along similar rationale.

Claims 3, 4, 7-10, 14,15, 17-20, 29, 32, 34, 43, and 46, are rejected under 35 U.S.C. 103(a) as being unpatentable over Kim et al. World Intellectual Property Organization No. WO 03/050784 (hereinafter Kim) International Filing Date 17 April 2002 in view of Luyster U.S. Patent No. 6,751,319 (hereinafter Luyster) in further view of 3GPP TS 35.202 v3.1.1 Release 1999 (hereinafter 3GPP) in further view of Weybrew et al. U.S. Patent No. 6,931,511 (hereinafter Weybrew).

Regarding claim 3, the following is not explicitly taught in GPP, Kim and Luyster: "wherein for each look-up table, the plurality of elements of the look-up table and the plurality of

inputs are loaded as vectors and the looking-up comprises, for each of the inputs selecting one of the plurality of elements of the look-up table using the first set of bits that define the input" however Weybrew teaches a plurality of look-up tables being loaded as vectors in col. 8, lines 37-56.

Regarding claim 4, "comprising using a vperm (vector permutation) instruction for selecting one of the plurality of elements of the look-up table using the first set of bits that define the input" however Weybrew teaches a vperm instruction in col. 29, lines 44-67.

Regarding claim 7, "wherein for each time the selection on a remaining number of corresponding outputs is performed, the remaining number of corresponding outputs comprises at least one set of two remaining corresponding outputs and the selection of half of the remaining number of outputs comprises, for each set of two corresponding outputs of the at least one set of two remaining corresponding outputs:" is shown in Kim page 2, lines 25-36;

"replicating the respective bit into a plurality of replicated bits; and using a vector instruction, selecting one of the two remaining corresponding outputs depending on the plurality of replicated bits" however Weybrew teaches utilizing vectors to select outputs in col. 8, lines 56-65.

Regarding claim 8, "wherein the vector instruction is a vsel (vector select instruction)" however Weybrew shows a method to lookup data items indexed by a plurality of vectors in col. 8, lines 56-65.

Regarding claim 9, "wherein for each input, the first set of bits that define the input comprises five bits, the second set of bits that define the input comprises two bits and the look-up

tables comprise four look-up tables, wherein for each of the four look-up tables the plurality of inputs and the plurality of elements of the look-up table are loaded as vectors and the looking-up comprises for each of the inputs selecting one of the plurality of elements of the look-up table using the first set of bits that define the input" however Weybrew teaches vectors are loaded in a plurality of lookup tables in col 8, lines 37-67.

Regarding claim 10, "wherein for each input, the first set of bits that define the input comprises four bits, the second set of bits that define the input comprises three bits and the look-up tables comprise eight look-up tables, and wherein for each of the eight look-up tables the plurality of inputs and the plurality of elements of the look-up table are loaded as vectors and for each of the inputs the looking-up comprises selecting one of the plurality of elements of the look-up table using the first set of bits that define the input" however Weybrew teaches that the vector are indices in col. 8, lines 37-56.

Regarding claims 14, 15, 17-20, these claims contain substantially similar subject matter as claims 3, 4, 7-10; therefore they are rejected along similar rationale. Note an Altivec processor is shown in Weybrew col. 5, lines 36-46.

Regarding claim 29, "wherein for each input of the plurality of inputs, for each look-up table the respective subset of bits of the first plurality of bits that define the input comprises one of 4 and 5 bits and the look-up table is looked-up using a vperm (vector permutation) instruction" however Weybrew teaches a vperm instruction in col. 29, lines 44-67.

Regarding claim 32, "wherein the bit shifting instruction comprises one of a vector shift right byte instruction and a vector shift left byte instruction and the bit rotation instruction

comprises one of a vector rotate left byte instruction and a vector rotate right byte instruction" however Weybrew teaches in col. 80, lines 17-41 a macro to rotate vector.

(10) Response to Argument

Regarding appellant's argument beginning on page 10, "Claims 74-76 are directed to the simultaneous use of different parts of a signal to address one or more lookup tables … but the novelty in claim 74 is not simply the use of a lookup table but the parallel use of different parts of a single input signal to address different lookup tables or different parts of a lookup table … At page 6 of the final Office action, the examiner reads the upper 16 bits and the lower 16 bits of the 32-bit input in Kim as the claimed plurality of inputs, but this is unreasonable reading of the claim language and Kim et al. There is only one input in Kim et al 32-bit input. The upper and lower sets of bits are different parts of the same input, but are not a plurality of inputs as required in claims 74-76 … The result is that Kim et al uses two different parts of a single input and uses them in series, whereas the present invention uses different inputs and uses them in parallel".

The Examiner disagrees with the argument it is the combination of references that teaches the claimed and argued feature. As taught in Kim the Kasumi encryption algorithm is utilized. Note Applicant's disclosure, i.e. Abstract states the following: "A method and apparatus are used to generate outputs according to a ciphering algorithm ... An example parallel implementation involves the Kausmi algorithm in which S7 and S9 function are evaluated in parallel". Therefore it is interpreted that the plurality of inputs is equivalent to the plurality of bits utilized with the Kasumi encryption algorithm. This interpretation is consistent with the Applicant's disclosure. It is known in the art that the Kasumi encryption algorithm divides the input into sections and

that the different sections are processed in parallel, see Kim page 3, lines 12-29, which describes the 'three-stage pipeline structure' 'the output data of the pipeline register section so that the output data of the FO block and the FL2 block are synchronized'. In addition Kim teaches the use of a multistage pipeline using a plurality of pipeline registers, see page 2 ones 26-33. The Examiner interprets the plurality of bits equivalent to a plurality of inputs. Note the lookup tables are defined by Luyster as s-boxes used for symmetric encryption systems see col. 4, lines 54-67. Therefore it is understood that Kim teaches the use of s-boxes or registers (look-up-tables) for storing secret keys see page 11, lines 1-13. In addition it is understood that Kim teaches the claimed invention "for each first input and in parallel with other first inputs of the plurality of first inputs", "FO block and the FL2 block are synchronized", Note synchronized is parallel or concurrently as described by applicants disclosure, as well as page 16 of Kim which states "Also, by combining in parallel two or more encryption apparatuses diversely implement as described above", therefore Kim teaches parallel use of inputs.

Regarding appellant's argument beginning on page 11, "Thus, the additional reference does not make up for the deficiencies already pointed out relative to Kim and Luyster ...for the same reasons"

As stated above there are no deficiencies with the Kim and Luyster combination teaching the claimed invention. Note, Kim teaches the use of the Kasumi encryption algorithm in apparatus that can be applied to portable terminals. Luyster teaches a block cipher method that includes a computing unit using a plurality of rounds and s-box. The combination of Kim and Luyster explicitly teaches the claimed use of look-up tables with the encryption apparatus is equivalent to

s-boxes.

The combination of Kim, Luyster with 3GPP is to explicitly teach "and selecting a corresponding output from the set of corresponding outputs using the second set of at least one bit that defines the input". Note Kim also discusses the 3GPP in the background page 1, lines 10-23.

Regarding appellant's argument on page 13, "In the final Office action, the examiner again refers to the upper and lower bits as first and second sets of bits, but the examiner has missed the point. Claim 1 requires that there be plural inputs, with each input defined by the first and second sets of bits. The upper and lower sets of bits in Kim et al are different parts of the same input … there are two steps performed. First, the first set of bits of the plurality of inputs are used to access plural lookup tables with the outputs from the …. Second, the second set of bits of each input is used to select one output from the set of outputs. These two steps are performed for each input, and in parallel with other inputs".

The Examiner disagrees with the Applicant's argument, first as explained above the Applicant's disclosure states the claimed invention is to improve the Kasumi encryption algorithm implementation, see Applicant's abstract. In addition as shown in Applicant's disclosure paragraph 8, "one parallel implementation involves the Kasumi algorithm in which S7 and S9 functions are evaluated in parallel for a plurality of inputs using vector instruction on a Single Instruction Multiple Data architecture. Note Kim is directed to apparatus applying a Kasumi encryption algorithm in a multistage pipeline, see Kim abstract. In addition Kim teaches

simultaneously stores outputs of the pipeline registers applicable to the S7 and S9 Kasumi functions on page 9. Kim teaches the claimed invention.

Regarding appellant's argument beginning on page 13, "Section IV at page 4, the examiner dismisses these arguments on multiple unsupportable grounds. First, the examiner argues that claim 1 does not require multiple lookup tables … The examiner further argues that the Kasumi algorithm uses plural inputs, but this does not lead to the use of plural lookup tables in particular manner recited in claim 1".

The Examiner disagrees with argument. Note claim 1 in its entirety is shown below:

> 1. (previously presented) A method comprising, responsive to a plurality of inputs, each input being defined by a first set of bits and a second set of at least one bit, for each input of the plurality of inputs and in parallel with other inputs of the plurality of inputs:
>
> looking-up one of a plurality of elements of each of a plurality of look-up tables using the first set of bits that define the input to obtain an output, the outputs from each of the plurality of look-up tables collectively comprising a set of corresponding outputs; and
>
> selecting a corresponding output from the set of corresponding outputs using the second set of at least one bit that defines the input.

Based on Applicant's disclosure, see paragraphs 5 and 7, "The Kasumi algorithm including evaluation of the S7 and S9 function have not been implemented in parallel for multiple inputs … with each look-up table being looked-up in parallel using respective inputs … The methods allows the ciphering algorithm to be implemented partially or entirely in parallel". Therefore, it is understood, claim 1 is directed to implementation of Kasumi algorithm where a plurality of

inputs i.e. bits split in the S7 or S9 functions (s-Box equivalent to lookup table Luyster) are utilize look-up tables to select an output. Kim teaches the same features in a multistage pipeline. The initial bits are split and the output chosen based on inputs, see Abstract and page 9. Note the F1 function defined in Kasumi encryption algorithm as well as 'simultaneously stores' and operating on the inputs in the multistage pipeline are all taught in the combination of references Kim, Luyster, and 3GPP.

Regarding appellant's argument on page 14, "In Section V at page 5, the examiner purports to dismiss applicants arguments, but the dismissal is not warranted … Claim 1 describes the use of the first parts of plural inputs to access plural lookup tables to generate a plurality of lookup tables outputs, and then the second part of each input being used to select one the set of outputs".

The Examiner disagrees with argument, the combination of references Kim, Luyster, and 3GPP teaches the claimed invention. Note Kim teaches apparatus for applying the Kasumi encryption algorithm. Luyster teaches a block cipher method and used to support concepts known within the art, i.e. s-boxes are lookup tables. 3GPP incorporated by reference in Kim teaches the basic concepts of the Kasumi encryption algorithm. The argued features above

'use of the first parts to access lookup tables ...

then second part of each input used to select one the set of outputs' is the Kasumi encryption algorithm. Specifically review 3GPP,

note page 7 “Kasumi is a block cipher that produces a 64-bit output from a 64-bit input under the control of a 128-bit key”,

note page 8, “Kasumi decomposes into a number of subfunctions (FL, FO, FI) which are used in conjunction with associated subkeys (KL, KO, KI) in a Feistel structure comprising a number of rounds (and rounds within rounds for some subfunctions)”

note page 9, “S7[] – An S-Box translating a 7-bit input to a 7-bit output. S9[] - An S-Box translating a 9-bit input to a 9-bit output ... Kasumi is Feistel cipher cipher with eight rounds"

note page 11, “4.4 Function FI … The function uses two S-boxes, S7 which maps a 7-bit input to a 7-bit out, and S9 which maps a 9-bit input to a 9-bit output”

note page 12, “4.5 S-boxes The two S-boxes have been designed so that they may be easily implemented in combination logic as well as by a look-up table”

Note Kasumi uses the input to select the output. In addition see Kim which uses a multistage pipeline to apply Kasumi encryption, see page 16 which states "Also, by combining in parallel two or more encryption apparatuses diversely implements as described above according, to the present invention, a multiple encryption apparatus that can encrypt different text data can be implemented. Industrial Applicability As apparent from the above description, according to the encryption apparatus applying a Kasumi encryption algorithm according to the present invention ... Thus, the encryption apparatus has a low power consumption, and is small-sized in comparison to the conventional encryption apparatus". The Applicant is arguing the basic concepts of the Kasumi encryption algorithm which are taught in the combination of references.

(11) Related Proceeding(s) Appendix

No decision rendered by a court or the Board is identified by the examiner in the Related Appeals and Interferences section of this examiner's answer.

For the above reasons, it is believed that the rejections should be sustained.

Respectfully submitted,

/ELLEN TRAN/

Primary Examiner, Art Unit 2433

Conferees:

/Brandon S Hoffman/

Primary Examiner, Art Unit 2433

/VIVEK SRIVASTAVA/

Supervisory Patent Examiner, Art Unit 2433